

## Sum-free sets and short covering codes

Emerson L. Monte Carmelo\*

Candido F. X. de Mendonça Neto†

### Abstract

Sum-free sets and some of their applications to number theory and Ramsey theory are reported. We also outline a recent link between sum-free sets and the numbers induced by short coverings. Given a prime power  $q$ , define  $c(q)$  as the minimum cardinality of a subset  $H$  of  $\mathbb{F}_q^3$  which satisfies the following property: every vector in this space differs in at most 1 coordinate from a multiple of a vector in  $H$ . We state two extremal problems aiming to discuss a known connection between the corresponding coverings and sum-free sets, which yield classes of coverings.

## 1 Introduction

Let  $\mathbb{F}_q^3$  denote the set of all vectors  $x = (x_1, x_2, x_3)$  with length 3 and components  $x_i$  taken on the field  $\mathbb{F}_q$  with  $q$  elements, where  $q$  is a prime or a prime power. This set becomes a metric space by defining the *Hamming distance*  $d(x, y)$  between the words  $x$  and  $y$  as the number of components in which  $x$  and  $y$  differ.

A subset  $C$  in  $\mathbb{F}_q^3$  is a *covering* of  $\mathbb{F}_q^3$  iff for every vector  $x$  in  $\mathbb{F}_q^3$ , there is a vector  $y$  in  $C$  such that  $d(x, y) \leq 1$ . The number  $K_q(3, 1)$  denotes the minimum cardinality of a covering of  $\mathbb{F}_q^3$ . Kalbfleish and Stanton [3], in 1969, showed that  $K_q(3, 1) = \lceil q^2/2 \rceil$ . The generalization for higher dimensions

---

2000 *AMS Subject Classification*. 11B75, 94B65, 05C55

*Key Words and Phrases*: covering code, extremal problem, sum-free set, cyclic group.

\*Partially supported by CNPq and Fundação Araucária - PR.

†Partially supported by CNPq.

and arbitrary radius (see [1]) has been extensively investigated by many researchers since the paper by Taussky and Todd [9] in 1948, see [4], for instance. An overview on covering codes is presented in [2]. Updated tables on these generalized numbers are available in Kéri [5].

A closely related problem is described below. A subset  $H$  of  $\mathbb{F}_q^3$  is a *short covering* of  $\mathbb{F}_q^3$  when  $\mathbb{F}_q \cdot H = \{\alpha \cdot h : \alpha \in \mathbb{F}_q \text{ and } h \in H\}$  is a covering of  $\mathbb{F}_q^3$ , where  $\alpha \cdot h$  denotes the scalar multiplication of  $h$  by  $\alpha$ . The induced extremal problem  $c(q)$  is defined as the minimum cardinality of such subset  $H$ . Both problems can be reformulated as dominating sets in the context of graph theory. The best bounds known on  $c(q)$  are

$$\left\lceil \frac{q+1}{2} \right\rceil \leq c(q) \leq \frac{3(q+4)}{4},$$

for  $q \geq 5$ , according to [7].

A known connection between the corresponding coverings and sum-free sets is reported. On the basis of this link, the contribution [6] introduces two extremal problems in combinatorial number theory aiming to provide the following upper bound.

**Theorem 1.1.** *Let  $q$  be a prime number or a prime power.*

1. *If  $q$  is odd, then  $c_q(3, 1) \leq 6 \left\lceil \frac{q-1}{12} \right\rceil + 6 \left\lceil \log_4\left(\frac{q-1}{4}\right) \right\rceil + 3$ ;*
2. *If  $q$  is even, then  $c_q(3, 1) \leq 6 \left\lceil \frac{q-1}{9} \right\rceil + 6 \left\lceil \log_4\left(\frac{q-1}{3}\right) \right\rceil + 3$ .*

It is worth mentioning that short coverings have been generalized for higher dimensions too, and relationships with the well-known numbers  $K_q(n, R)$  have been obtained.

This note is organized as follows. We outline briefly sum-free sets and a few of their remarkable applications in Section 2. A recent construction of short coverings based on sum-free sets is described in Section 3. Two combinatorial functions are discussed in order to prove Theorem 1.1.

## 2 Sum-free sets

Sum-free sets have been studied in several contexts and aspects, in connection with several branches of mathematics. In this section let us review some of the important applications.

### 2.1 a link with Number theory

One of the most famous problems of mathematics is the Fermat's last theorem, which states that there is not a non trivial (every variable is non-null) solution of the diophantine equation

$$x^m + y^m = z^m \quad (2.1)$$

for  $m \geq 3$ .

Among the many attempts of attack, the Dicksons strategy investigated the solutions of the above equation in the context of modular arithmetic  $\mathbb{Z}_p$ , for a prime  $p$ . Indeed, if there were not solution of (2.1) in  $\mathbb{Z}_p$  for any prime  $p$ , then there would not be solution of the original equation (2.1). The hope was broken in 1909 when Dickson himself showed that

**Theorem 2.1.** *(Dickson) If  $p$  is prime number sufficiently large, then the equation (2.1) admits a non trivial solution in  $\mathbb{Z}_p$ .*

In 1916, Schur offered a simple but nice proof of the Dicksons result. His proof is available in [8] or [10]. Let us describe here an important concept used in his insight.

A subset  $S$  of an (additively written) abelian group  $G$  is *sum-free* if no  $a, b, c$  in  $S$  satisfy the equation  $a + b = c$ , that is,  $(S + S) \cap S = \emptyset$ , where

$$S + S = \{a + b : a \in S \text{ and } b \in S\}.$$

For instance, let  $S = \{5, 6, 7, 8\}$  in  $\mathbb{Z}_{13}$ . Note that  $S + S = \{10, 11, 12, 0, 1, 2, 3\}$ , thus the sum of any two elements in  $S$  is never a element in  $S$ , that is,  $S$  is sum-free set in  $\mathbb{Z}_{13}$ .

The Schur number  $S(n)$  denotes the largest positive integer  $m$  such that there is a partition of  $\{1, 2, \dots, m\}$  into  $n$  subsets, each of which is sum-free.

For instance, the sum-free sets  $\{1, 4\}$  and  $\{2, 3\}$  yield a partition of  $\{1, 2, 3, 4\}$ , thus  $S(2) \geq 4$ . On the other hand, we claim that any partition of  $\{1, 2, 3, 4, 5\}$  into two subsets, say  $A$  and  $B$ , at least one of them is not sum-free. Indeed, because  $1 + 1 = 2$ ,  $2 + 2 = 4$ , and  $1 + 3 = 4$ , we can suppose that  $\{1, 4\} \subset A$  and  $\{2, 3\} \subset B$ . If  $5 \in A$  or  $5 \in B$ , then  $A$  or  $B$  is not sum-free, respectively. Therefore  $S(2) = 4$ .

**Theorem 2.2.** (Schur-1919) For any  $n \geq 1$ ,  $S(n) \leq n!e$ , where  $e = 2,718\dots$  denotes the base of the natural logarithms and  $n!$  represents the factorial of  $n$ .

*Proof:* See proof in [8] or [10]. ■

The exact values are known only for  $n = 1, 2, 3, 4$ , and the computation of  $S(n)$  still remains an open problem.

## 2.2 a link with Ramsey theory

The connection with the generalized Ramsey numbers for graphs is another important and nice application.

Let  $K_n$  denote the complete graph on  $n$  vertices. The Ramsey number  $R_r(3)$  denotes the smallest integer  $n$  such that for any  $r$ -coloring of the edges of  $K_n$ , one can always find a monochromatic subgraph isomorphic to the triangle  $K_3$ .

A simple argument shows that  $R_2(3) = 6$ . The number  $R_3(3) = 17$  is the only nontrivial Ramsey number known for more than two colors, obtained by Greenwood and Gleason by using certain sum-free sets. Moreover, a class of  $K_3$ -free graphs was constructed in 1966 by using sum-free sets, which implies the lower bound below.

**Theorem 2.3.** (Abbot and Moser-1966) For any  $r$ , we have  $R_r(3) \geq S(r) + 2$ .

*Proof:* See proof in [8] or [10]. ■

### 3 Tool 1: From sum-free sets to short coverings

A recent application of sum-free sets into combinatorial coding theory is described in this section.

A *family*  $\mathcal{P}$  is a subset of  $G \times G$ . Given a family  $\mathcal{P} = \{(a_1, b_1), \dots, (a_k, b_k)\}$  of  $G \times G$ , write

$$\Delta_{\mathcal{P}} = \{0\} \cup \bigcup_{i=1}^k \Delta(a_i, b_i),$$

where  $\Delta(a, b)$  denotes the subset  $\{a, b, -a, -b, a - b, b - a\}$  of  $G$ .

As usual,  $h^{S_3} = \{h^\alpha : \alpha \in S_3\}$  denotes the orbit of the vector  $h \in \mathbb{F}_q^3$  on the standard action of  $S_3$ . In particular,

$$(1, x, y)^{S_3} = \{(1, x, y), (1, y, x), (x, 1, y), (x, y, 1), (y, 1, x), (y, x, 1)\},$$

which has size 6 whenever 1,  $x$ , and  $y$  are pairwise distinct.

**Theorem 3.1.** [7] *Let  $\mathcal{P} = \{(\overline{a_1}, \overline{c_1}), \dots, (\overline{a_k}, \overline{c_k})\}$  be family in  $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$  and let  $\xi$  be a generator of the cyclic group  $\mathbb{F}_q^*$ . If the complement of  $\Delta_{\mathcal{P}}$  is sum-free in  $\mathbb{Z}_{q-1}$ , then the set*

$$H = (0, 1, 1)^{S_3} \cup \bigcup_{i=1}^k (1, \xi^{a_i}, \xi^{c_i})^{S_3}$$

*is a short covering of  $\mathbb{F}_q^3$ .*

The upper bound in Theorem 1.1 is derived by investigating two extremal problems associated to the Theorem 3.1. One of them is described below.

**Definition 3.2.** *Given a prime power  $q$ , let*

$$f(q) = \min\{|\mathcal{P}| : \text{the complement of } \Delta_{\mathcal{P}} \text{ is sum-free in } \mathbb{Z}_{q-1}\}.$$

Since the orbit  $(0, 1, 1)^{S_3}$  has three elements and any other orbit  $(1, \xi^a, \xi^c)^{S_3}$  has at most 6 elements, an immediate consequence of Theorem 3.1 is the inequality

$$c(q) \leq 6f(q) + 3, \tag{3.1}$$

which provides us a systematic way of constructing short coverings from the new mapping  $f(q)$ . On the other hand, upper bounds on  $f(q)$  are obtained by using a closely related mapping  $\delta$  introduced in the next section.

## 4 Tool 2: $\delta$ -covering

Consider two pairs:  $(5, 4)$  and  $(5, 3)$ . Note that  $5 - 4 = 1$  and  $5 - 3 = 2$ . Each element in  $[5] = \{1, 2, 3, 4, 5\}$  appears as a coordinate or is a difference of type  $a - b$ . Thus we say that  $\mathcal{P} = \{(5, 4), (5, 3)\}$  is a  $\delta$ -covering of  $[5]$ .

We formalize now this concept in a general context. Let  $(G, +)$  be an abelian group written in additive notation. For a family  $\mathcal{P} = \{(a_1, b_1), \dots, (a_k, b_k)\}$  of  $G \times G$ , let

$$\delta_{\mathcal{P}} = \bigcup_{i=1}^k \delta(a_i, b_i),$$

where  $\delta(a, b)$  denotes the subset  $\{a, b, a - b\}$  of  $G$ .

Given a subset  $U$  of  $G$  and a family  $\mathcal{P}$  in  $U \times U$ ,  $\mathcal{P}$  is a  $\delta$ -covering of  $U$  (or  $\mathcal{P}$   $\delta$ -covers  $U$ ) if  $U \subset \delta_{\mathcal{P}}$ .

In contrast with a partition used in the Schur number  $S(n)$ , every pair  $(a, b)$  of a family induces a non sum-free set  $\delta(a, b) = \{a, b, a - b\}$ .

Consider now the following extremal problem induced by the particular case where  $G = \mathbb{Z}$  and  $U = [n] = \{1, 2, \dots, n\}$ .

**Definition 4.1.** *Given a positive integer  $n$ , let*

$$\delta(n) = \min\{|\mathcal{P}| : \mathcal{P} \text{ is a } \delta\text{-covering of } [n] \text{ in } \mathbb{Z}\}.$$

This mapping plays the central role in our investigations because upper bounds on  $f$  will be obtained from properties of  $\delta$ . Trivial inequalities for  $n \geq 2$  are

$$\left\lceil \frac{n}{3} \right\rceil \leq \delta(n) \leq \frac{n}{2}. \quad (4.1)$$

**Example 4.2.** *An application of the previous lower bound yields  $\delta(12) \geq 4$ . Since  $\mathcal{P} = \{(12, 10), (11, 8), (9, 5), (7, 6)\}$  is a  $\delta$ -covering of  $[12]$  in  $\mathbb{Z}$ , the exact value  $\delta(12) = 4$  follows.*

**Proposition 4.3.** *The following upper bound holds for  $n \geq 2$ :*

$$\delta(n) \leq \lceil n/3 \rceil + \lceil \log_4(n) \rceil.$$

*Proof:* The proof is based on a recursive construction, according to [6]. ■

On the basis of the previous results, we are ready to construct sharper families of short coverings.

**Theorem 4.4.** *Let  $q$  be a prime power.*

1. *if  $q \equiv 1 \pmod{4}$ , then  $f(q) \leq \delta((q-1)/4)$ .*
2. *if  $q \equiv 3 \pmod{4}$ , then  $f(q) \leq \delta((q-3)/4)$ .*
3. *if  $q = 2^r$  with  $q \equiv 1 \pmod{3}$ , then  $f(q) \leq \delta((q-1)/3)$ .*
4. *if  $q = 2^r$  with  $q \equiv 2 \pmod{3}$ , then  $f(q) \leq \delta((q-2)/3)$ .*

*Proof:* The proof combines homomorphism of cyclic groups and constructive methods for  $\delta$ -coverings, see details in [6]. ■

**Example 4.5.** *We exhibit the above construction for  $q = 49$ . By using the homomorphism  $x \rightarrow \bar{x}$  of  $\mathbb{Z}$  into  $\mathbb{Z}_{24}$ , the family  $P$  given in Example 4.2 generates the family*

$\bar{P} = \{(\overline{12}, \overline{10}), (\overline{11}, \overline{8}), (\overline{9}, \overline{5}), (\overline{7}, \overline{6})\}$ . Note that  $\Delta(\overline{12}, \overline{10}) = \{\overline{12}, \overline{10}, \overline{2}, \overline{14}, \overline{22}\}$ ,  $\Delta(\overline{11}, \overline{8}) = \{\overline{11}, \overline{8}, \overline{3}, \overline{13}, \overline{16}, \overline{21}\}$ ,  $\Delta(\overline{9}, \overline{5}) = \{\overline{9}, \overline{5}, \overline{4}, \overline{15}, \overline{19}, \overline{20}\}$ , and  $\Delta(\overline{7}, \overline{6}) = \{\overline{7}, \overline{6}, \overline{1}, \overline{17}, \overline{18}, \overline{23}\}$ . Therefore  $\Delta_{\bar{P}} = \mathbb{Z}_{24}$ . By using the homomorphism  $\bar{x} \rightarrow \overline{2x}$  of  $\mathbb{Z}_{24}$  into  $\mathbb{Z}_{48}$ , the set  $P^* = \{(\overline{24}, \overline{20}), (\overline{22}, \overline{16}), (\overline{18}, \overline{10}), (\overline{14}, \overline{12})\}$  in  $\mathbb{Z}_{48}$  satisfies  $\Delta_{P^*} = \{\overline{0}, \overline{2}, \overline{4}, \dots, \overline{46}\}$ . Since its complement  $\mathbb{Z}_{48} - \Delta_{P^*}$  is sum-free in  $\mathbb{Z}_{48}$ , the value  $f(49) \leq 4$  follows. By Eq. (3.1), we obtain  $c(49) \leq 27$ , improving the previous bound  $c(49) \leq 39$ .

*Proof of Theorem 1.1:* The proof is an application of Eq. (3.1), Theorem 4.4, and Proposition 4.3. ■

**Acknowledgments:** The authors thank the referees for careful readings and suggestions.

## References

- [1] W.A. Carnielli, *On covering and coloring problems for rook domains*, Discrete Math. 57 (1985), 9–16.
- [2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam (1997).
- [3] J.G. Kalbfleish and R.G. Stanton, *A combinatorial problem in matching*, J. London Math. Soc. 44 (1969), 60–64.
- [4] W. Haas, J.C.S Puchta, and J. Quistorff, *Lower bounds on covering codes via partition matrices*, J. Combin. Theory Ser A (2009), 478–484.
- [5] G. Kéri, tables for bound on covering codes, accessed (2011), homepage: <http://www.sztaki.hu/~keri/>.
- [6] E.L. Monte Carmelo and C.F.X. De Mendonça Neto, *Extremal problems on sum-free sets and coverings in tridimensional spaces*, Aequationes Mathematicae 78 (2009), 101–112.
- [7] E.L. Monte Carmelo and I.N. Nakaoka, *Short coverings in tridimensional spaces arising from sum-free sets*, European J. Combin. 29 (2008), 227–233.
- [8] A. Soifer, *The mathematical coloring book*, Springer, New York (2009).
- [9] O. Tauskky and J. Todd, *Covering theorems for groups*, Ann. Soc. Polonaise Math. 21 (1948), 303–305.
- [10] W.D. Wallis, A.P. Street, and J.S. Wallis, *Combinatorics: room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics, vol. 292, Springer-Verlag, Berlin-Heidelberg-New York (1972).

Emerson L. Monte Carmelo  
Departamento de Matemática

Universidade Estadual de Maringá  
87020-900, Maringá, PR,  
Brazil  
e-mail: elmcarcelo@uem.br

Candido F. X. de Mendonça Neto  
Escola de Artes, Ciências  
e Humanidades,  
Universidade de São Paulo  
São Paulo, SP,  
Brazil  
e-mail: cfxavier@usp.br